Refine Search

Search Results -

Terms	Documents
709/227	5199

Database:
US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search:

Refine Search

Recall Text

Clear

Interrupt

Search History

DATE: Saturday, September 17, 2005 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR			
L32	709/227	5199	L32
L31	709/218	4167	L31
L30	709/217	6999	L30
L29	713/201	6079	L29
L28	713.clas.	22111	L28
L27	726/3	0	L27
L26	726/1	0	L26
L25	726.clas.	7014	L25
L24	709.clas.	39230	L24
L23	709/246	2221	L23
L22	709/229	4918	L22
L21	709/206	4548	L21
L20	707/9	2461	L20
L19	l18 and (admin or administrative) with domain	160	L19
L18	L17 and group with users	910	L18
L17	(database or data with base) near directory	2682	L17
L16	L14 and (admin or administrative) with (priviledges or rights)	17	L16

L15	L14 and (admin or administrative) with priviledges	0	L15
L14	L13 and group near users	176	L14
L13	manag$ near user near information	1419	L13
L12	6311194.pn.	2	L12
L11	6233586.pn.	2	L11
L10	707/10	10473	L10
L9	707/4	4293	L9
L8	707/505	416	L8
L7	715/505	190	L7
L6	707/103	3582	L6
L5	707.clas.	29272	L5
L4	707/2	4612	L4
L3	707/6	3072	L3
L2	707/1	7019	L2
L1	707/100	6597	L1

END OF SEARCH HISTORY

L19: Entry 121 of 160 File: PGPB Jul 18, 2002

PGPUB-DOCUMENT-NUMBER: 20020095499
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020095499 A1

TITLE: Delegated administration of information in a database directory using attribute permissions

PUBLICATION-DATE: July 18, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Barnett, Janet Arlie	Pattersonville	NY	US	
Vivier, Barbara Jean	Niskayuna	NY	US	
Aggour, Kareem Sherif	Schenectady	NY	US	
Kornfein, Mark Mithchell	Latham	NY	US	
Oksoy, Osman Rifki	Clifton Park	NY	US	
Williams, Bassel Omari	Albany	NY	US	
Sebastian, Jose	Waukesha	WI	US	
Mehring, David Thomas	Sussex	WI	US	

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	COUNTRY	TYPE CODE
General Electric Company with cover sheet				02

APPL-NO: 09/ 760999 [PALM]
DATE FILED: January 16, 2001

INT-CL: [07] G06 F 15/173

US-CL-PUBLISHED: 709/226; 709/223
US-CL-CURRENT: 709/226; 709/223

REPRESENTATIVE-FIGURES: 1

ABSTRACT:

A delegated administrative tool for administrating information in a database directory using attribute permissions. The delegated administrative tool enables an administrator to form administrative domains and sub-domains having user attribute permissions that define administrative operations that an administrator can and cannot perform on a user attribute. Also, the delegated administrative tool enables an administrator to define restricted values for assigning to the user attributes.

L19: Entry 122 of 160 File: PGPB Jul 18, 2002

PGPUB-DOCUMENT-NUMBER: 20020095414
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020095414 A1

TITLE: Delegated administration of information in a database directory

PUBLICATION-DATE: July 18, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Barnett, Janet Arlie	Pattersonville	NY	US	
Vivier, Barbara Jean	Niskayuna	NY	US	
Aggour, Kareem Sherif	Schenectady	NY	US	
Kornfein, Mark Mitchell	Latham	NY	US	

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	COUNTRY	TYPE CODE
General Electric Company				02

APPL-NO: 09/ 761000 [PALM]
DATE FILED: January 16, 2001

RELATED-US-APPL-DATA:
Application is a non-provisional-of-provisional application 60/241645, filed October 19, 2000,

INT-CL: [07] G06 F 7/00

US-CL-PUBLISHED: 707/9
US-CL-CURRENT: 707/9

REPRESENTATIVE-FIGURES: 4

ABSTRACT:

A delegated administration tool for administrating information in a database directory. The delegated administration tool enables an administrator to delegate administration and various types of administrative authority to other users within a community of users. In particular, an administrator with proper authority may create new administrative domains and assign authority referred to as delegation authority and edit authority to other users. The creation of additional administrative domains and the assignment of the delegation authority and edit authority can continue to an arbitrary level within the community.

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Application Serial No. 60/241,645 filed on Oct. 19, 2000, and entitled "Approach And Design For Software To Facilitate Delegated Administration Of Information In A Database Directory," which is incorporated by reference herein in its entirety.

Previous Doc Next Doc Go to Doc#

Hit List

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Search Results - Record(s) 121 through 130 of 160 returned.

☐ 121. Document ID: US 20020095499 A1

Using default format because multiple data bases are involved.

L19: Entry 121 of 160 File: PGPB Jul 18, 2002

PGPUB-DOCUMENT-NUMBER: 20020095499
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020095499 A1

TITLE: Delegated administration of information in a database directory using attribute permissions

PUBLICATION-DATE: July 18, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Barnett, Janet Arlie	Pattersonville	NY	US	
Vivier, Barbara Jean	Niskayuna	NY	US	
Aggour, Kareem Sherif	Schenectady	NY	US	
Kornfein, Mark Mithchell	Latham	NY	US	
Oksoy, Osman Rifki	Clifton Park	NY	US	
Williams, Bassel Omari	Albany	NY	US	
Sebastian, Jose	Waukesha	WI	US	
Mehring, David Thomas	Sussex	WI	US	

US-CL-CURRENT: 709/226; 709/223

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw Desc | Image

☐ 122. Document ID: US 20020095414 A1

L19: Entry 122 of 160 File: PGPB Jul 18, 2002

PGPUB-DOCUMENT-NUMBER: 20020095414
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020095414 A1

TITLE: Delegated administration of information in a database directory

PUBLICATION-DATE: July 18, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Barnett, Janet Arlie	Pattersonville	NY	US	
Vivier, Barbara Jean	Niskayuna	NY	US	
Aggour, Kareem Sherif	Schenectady	NY	US	

Kornfein, Mark Mitchell Latham NY US

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	COUNTRY	TYPE CODE
General Electric Company				02

APPL-NO: 09/ 761000 [PALM]
DATE FILED: January 16, 2001

RELATED-US-APPL-DATA:
Application is a non-provisional-of-provisional application 60/241645, filed October 19, 2000,

INT-CL: [07] G06 F 7/00

US-CL-PUBLISHED: 707/9
US-CL-CURRENT: 707/9

REPRESENTATIVE-FIGURES: 4

ABSTRACT:

A delegated administration tool for administrating information in a database directory. The delegated administration tool enables an administrator to delegate administration and various types of administrative authority to other users within a community of users. In particular, an administrator with proper authority may create new administrative domains and assign authority referred to as delegation authority and edit authority to other users. The creation of additional administrative domains and the assignment of the delegation authority and edit authority can continue to an arbitrary level within the community.

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Application Serial No. 60/241,645 filed on Oct. 19, 2000, and entitled "Approach And Design For Software To Facilitate Delegated Administration Of Information In A Database Directory," which is incorporated by reference herein in its entirety.

---

123. Document ID: US 20020066033 A1

L19: Entry 123 of 160 File: PGPB May 30, 2002

PGPUB-DOCUMENT-NUMBER: 20020066033
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020066033 A1

TITLE: Managing content resources

PUBLICATION-DATE: May 30, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Dobbins, Kurt A.	Bedford	NH	US	
Poirier, Jason P.	Bedford	NH	US	
Weiss, Wouter Johan	Chelmsford	MA	US	

Boutin, Andre C.	Manchester	NH	US
Haddad, Justin William	Merrimack	NH	US
Delahunty, Stephen G.	Bedford	NH	US
Cullerot, David L.	Nasha	NH	US
Sexton, Mark Thomas	Merrimack	NH	US
Lederman, Adam Michael	Nashua	NH	US
Cheetham, Christopher Lawrence	Auburn	NH	US
Ruffen, David	Salem	NH	US

APPL-NO: 09/ 918972 [PALM]
DATE FILED: July 31, 2001

RELATED-US-APPL-DATA:
Application is a non-provisional-of-provisional application 60/222038, filed July 31, 2000,

INT-CL: [07] H04 L 9/00

US-CL-PUBLISHED: 713/201
US-CL-CURRENT: 726/4

REPRESENTATIVE-FIGURES: 2

ABSTRACT:

Content resources are managed. A request is received from a user for access to a source of content resources. It is determined that the user is authorized for access to the source. A portal Web page is generated based on a set of content element data applicable to the subscriber. The portal Web page is returned to the user. A system for use in managing content resources has a switch for receiving requests from Web browsers, a content resource management engine in communication with the switch, and a billing system in communication with the content resource management engine.

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Application Serial No. 60/222,038 entitled "DIRECTORY-ENABLED BROADBAND SERVICE NETWORK," filed on Jul. 31, 2000, which is incorporated herein by reference.

☐ 124. Document ID: US 20020062451 A1

L19: Entry 124 of 160 File: PGPB May 23, 2002

PGPUB-DOCUMENT-NUMBER: 20020062451
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020062451 A1

TITLE: System and method of providing communication security

PUBLICATION-DATE: May 23, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Scheidt, Edward M.	McLean	VA	US	

Wack, C. Jay Clarksburg MD US

APPL-NO: 09/ 858326 [PALM]
DATE FILED: May 16, 2001

RELATED-US-APPL-DATA:
Application is a non-provisional-of-provisional application 60/098915, filed September 1, 1998,

Application is a non-provisional-of-provisional application 60/204385, filed May 15, 2000,

INT-CL: [07] H04 L 9/00, H04 L 9/32, G06 F 11/30, G06 F 12/14

US-CL-PUBLISHED: 713/201
US-CL-CURRENT: 726/7

REPRESENTATIVE-FIGURES: 1

ABSTRACT:

A process of checking the authorization and authenticity of an application provided by a user includes authenticating an application authentication file against a domain administrator's public membership key. An application executable is then hashed, and the application hash result is compared to an authentication hash contained in the application authentication file. At this point, services are denied to the application if the application hash and the authentication hash do not match. Configuration assignments in the application authentication file are decoded if the application hash and the authentication hash match. The decoded configuration assignments are compared to the user's configuration assignments. Services are provided to the application if the result of the decode is favorable. Services are denied to the application if the result of the decode is not favorable.

INCORPORATION BY REFERENCE

[0001] This document incorporates by this reference, the entire disclosures of the following U.S. patent applications and patents: 08/974,843 filed Nov. 20, 1997; 09/108,312 filed Jul. 1, 1998; 09/0123,672 filed Feb. 13, 1998; and 60/098,915 filed Sep. 1, 1998. This document also incorporates by reference U.S. Provisional Patent Application No. 60/204,385, which was filed on May 15, 2000.

☐ 125. Document ID: US 6941348 B2

L19: Entry 125 of 160 File: USPT Sep 6, 2005

US-PAT-NO: 6941348
DOCUMENT-IDENTIFIER: US 6941348 B2

TITLE: Systems and methods for managing the transmission of electronic messages through active message date updating

DATE-ISSUED: September 6, 2005

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Petry; Scott M.	Palo Alto	CA		
Akamine; Shinya	Menlo Park	CA		

Lund; Peter Kevin	San Francisco	CA
Cox; Fred	San Jose	CA
Oswall; Michael John	San Francisco	CA

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Postini, Inc.	Redwood City	CA			02

APPL-NO: 10/ 370118 [PALM]
DATE FILED: February 19, 2003

PARENT-CASE:
CROSS-REFERENCE TO RELATED APPLICATION This Application claims the benefit of U.S. Provisional Application Ser. No. 60/357,893, filed on Feb. 19, 2002, and entitled "E-Mail Management Services" commonly assigned with the present invention and incorporated herein by reference.

INT-CL: [07] G06 F 15/16

US-CL-ISSUED: 709/206; 709/224
US-CL-CURRENT: 709/206; 709/224

FIELD-OF-SEARCH: 709/223, 709/224, 709/202, 709/206, 709/229, 707/102, 715/530, 715/531

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
4837798	June 1989	Cohen et al.	
5619648	April 1997	Canale et al.	
5627764	May 1997	Schutzman et al.	
5634005	May 1997	Matsuo	
5742668	April 1998	Pepe et al.	
5796948	August 1998	Cohen	
5832208	November 1998	Chen et al.	
5844969	December 1998	Goldman et al.	
5889943	March 1999	Ji et al.	
5905777	May 1999	Foladare et al.	
5937162	August 1999	Funk et al.	
5968117	October 1999	Schuetze	
5987611	November 1999	Freund	
6014429	January 2000	LaPorta et al.	
6023723	February 2000	McCormack et al.	
6052709	April 2000	Paul	
6061718	May 2000	Nelson	
6073165	June 2000	Narasimhan et al.	
6075863	June 2000	Krishnan et al.	
6092194	July 2000	Touboul	
6112227	August 2000	Heiner	709/203
6146026	November 2000	Ushiku	
6178331	January 2001	Holmes et al.	
6249807	June 2001	Shaw et al.	

6263202	July 2001	Kato et al.	
6301245	October 2001	Luzeski et al.	
6317751	November 2001	Yeger et al.	707/104.1
6321267	November 2001	Donaldson	
6335966	January 2002	Toyoda	
6389276	May 2002	Brilla et al.	
6404762	June 2002	Luzeski et al.	
6411684	June 2002	Cohn et al.	
6434601	August 2002	Rollins	
6438215	August 2002	Skladman et al.	
6442589	August 2002	Takahashi et al.	
6453327	September 2002	Nielsen	
6487586	November 2002	Ogilvie et al.	709/206
6513045	January 2003	Casey et al.	
6574658	June 2003	Gabber et al.	709/206
6609196	August 2003	Dickinson, III et al.	
6615258	September 2003	Barry et al.	709/223
6654787	November 2003	Aronson et al.	
6711618	March 2004	Danner et al.	709/228
2001/0032095	October 2001	Balbach	

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
WO 96/35994	November 1996	WO	
WO 97/27546	July 1997	WO	
WO 98/37680	August 1998	WO	
WO 99/06929	February 1999	WO	
WO 00/49776	August 2000	WO	
WO 01/46867	June 2001	WO	

OTHER PUBLICATIONS

PCT International Preliminary Examination Report (PCT/US03/04757).
PCT Published Application WO 2003/071390 A2.
International Search Report, Form PCT/ISA/210 as found in PCT Application No. PCT/US03/04757 dated Apr. 14, 2004.
Http://web.archive.org/web/20000815053401/www.brightmail.com/corporate/ overview/.
Http://web.archive.org/web/19990128140052/http://www.chooseyourmail.com/.
Http://web.archive.org/web/20000815064559/www.commtouch.com/solutions/ index.shtml.
Http://web.archive.org/web/20001205151400/mailcircuit.com/route.htm.
Http://web.archive.org/web/20000824040241/www.messagelabs.com/about/ Overview/Overview.htm.
Http://web.archive.org/web/20000816134259/www.antivirus.com/products/ emai-groupware.htm.

ART-UNIT: 2144

PRIMARY-EXAMINER: Thompson; Marc D.

ATTY-AGENT-FIRM: Baker & McKenzie LLP

ABSTRACT:

The present invention provides an electronic message management system (EMS) that includes a real-time feedback loop where data is collected from the electronic messages on incoming

connection attempts, outgoing delivery attempts, and message content analysis, and written to a centralized data matrix. A separate process accesses the data matrix and analyzes trends in that data. The detected data patterns, trends or behavior is based on configuration parameters for the recipient. Based on these determinations, the process is able to instruct components in the EMS to accept, redirect, refuse, modify, defer, or otherwise dispose of the connection request, the delivery attempt, or the message. Associated methods for managing the transmission of electronic messages are also disclosed.

105 Claims, 18 Drawing figures

☐ 126. Document ID: US 6898595 B2

L19: Entry 126 of 160 File: USPT May 24, 2005

US-PAT-NO: 6898595
DOCUMENT-IDENTIFIER: US 6898595 B2

TITLE: Searching and matching a set of query strings used for accessing information in a database directory

DATE-ISSUED: May 24, 2005

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Vivier; Barbara Jean	Niskayuna	NY		
Aggour; Kareem Sherif	Schenectady	NY		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
General Electric Company	Niskayuna	NY			02

APPL-NO: 10/ 094894 [PALM]
DATE FILED: March 12, 2002

PARENT-CASE:
CROSS REFERENCE TO RELATED APPLICATIONS This application is a continuation-in-part of U.S. patent application Ser. No. 09/760,995, entitled "Delegated Administration Of Information In A Database Directory Using At Least One Arbitrary Group Of Users", filed Jan. 16, 2001, which claims the benefit of U.S. Provisional Application Ser. No. 60/241,645 filed on Oct. 19, 2000, entitled "Approach And Design For Software To Facilitate Delegated Administration Of Information In A Database Directory".

INT-CL: [07] G06 F 17/30

US-CL-ISSUED: 707/6
US-CL-CURRENT: 707/6

FIELD-OF-SEARCH: 707/6, 707/2

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL

5941947	August 1999	Brown et al.	
6067548	May 2000	Cheng	
6233586	May 2001	Chang et al.	707/103R
6311194	October 2001	Sheth et al.	715/505
6345266	February 2002	Ganguly et al.	707/1
6426955	July 2002	Gossett Dalton et al.	370/401
6513036	January 2003	Fruensgaard et al.	707/4
6539382	March 2003	Byrne et al.	707/10
6560595	May 2003	Sanders et al.	707/2

OTHER PUBLICATIONS

Oblix NetPoint 4.0 [online]. Oblix, Inc. [retrieved on Dec. 18, 2000]. Retrieved from the Internet:<URL:http://www.oblix.com/products_and _solutions/netpoint/>.
Securant Products [online]. Securant Technologies [retrieved on Dec. 18, 2000]. Retrieved from the Internet: <URL: http://www.securant.com/ie/main_products.html>.
Delegated Management Services [online]. Netegrity, Inc. [retrieved on Dec. 18, 2000]. Retrieved from the Internet: <URL: http://www.netegrity.com/products/dms.html>.
Iplanet Delegated Administrator 4.5 Datasheet [online]. iPlanet International [retrieved on Dec. 18, 2000]. Retrieved from the Internet:<URL: http://iplanet.com/products/infrastructure/dir_security/del_admin/>.

ART-UNIT: 2161

PRIMARY-EXAMINER: Amsbury; Wayne

ATTY-AGENT-FIRM: Fletcher Yoder

ABSTRACT:

Searching and matching a set of query strings used for accessing information in a database directory. In this disclosure, a user community administration tool queries a database directory containing user information associated with a user community. In the user community administration tool, there is an input query generation component that generates an input query having a search pattern that includes a combination of attribute names, logical, operators and attribute values. An accessing component accesses a library of queries used for accessing the user information in the database directory. A partitioning component partitions each of the queries in the library into logical units. Each logical unit comprises a combination of an attribute name, logical operator and attribute value. A comparing component compares the search pattern of the input query to each partitioned logical unit for each of the queries in the library. The comparing component compares the attribute name of the input query to the attribute name in the logical unit, the operator used in the input query to the operator used in the logical unit and the attribute value in the input query to the attribute value in the logical unit. A determining component determines whether there is a match between the input query and any of the logical units associated with each of the queries in the library.

29 Claims, 16 Drawing figures

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWMC | Draw Desc | Image

☐ 127. Document ID: US 6854016 B1

L19: Entry 127 of 160 File: USPT Feb 8, 2005

US-PAT-NO: 6854016
DOCUMENT-IDENTIFIER: US 6854016 B1

TITLE: System and method for a web based trust model governing delivery of services and

programs

DATE-ISSUED: February 8, 2005

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Kraenzel; Carl J.	Boston	MA		
Immerman; John D.	Sudbury	MA		
Mills; William A.	Arlington	MA		
Lu; Jeannie J.	West Roxbury	MA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
International Business Machines Corporation	Armonk	NY			02

APPL-NO: 09/ 596745 [PALM]
DATE FILED: June 19, 2000

PARENT-CASE:
CROSS REFERENCES TO RELATED APPLICATIONS The following U.S. patent applications filed concurrently herewith are assigned to the same assignee hereof, contain subject matter related, in certain respect, to the subject matter of the present application and are incorporated herein by reference: U.S. patent application Ser. No. 09/496,283 filed 19 Jun. 2000 for "System and Method for Providing a Distributable Runtime"; U.S. patent application Ser. No. 09/596,282 filed 19 Jun. 2000 for "System and Method for Downloading Security Context Elements Governing Execution of Downloadable and Distributable Agents"; U.S. patent application Ser. No. 09/596,963 filed 19 Jun. 2000 for "System and Method for Selective Replication of Databases Within a Workflow, Enterprise, and Mail-Enabled Web Application Server and Platform"; U.S. patent application Ser. No. 09/597,997 filed 19 Jun. 2000 for "System and Method For Providing a Distributable Runtime That Deploys Web Applications and Services From a Workflow, Enterprise, and Mail-Enabled Web Application Server and Platform"; U.S. patent application Ser. No. 09/596,783 filed 19 Jun. 2000 for "System and Method for Managing Concurrent Scheduled or On-demand Replication of Subscriptions"; and U.S. patent application Ser. No. 09/596,845 filed 19 Jun. 2000 for "A System and Method for Developing and Administering Web Applications and Services From a Workflow, Enterprise, and Mail-Enabled Web Application Server and Platform.

INT-CL: [07] G06 F 15/16

US-CL-ISSUED: 709/229; 709/217, 709/223, 709/224, 709/219, 713/155, 713/200, 717/172, 717/177
US-CL-CURRENT: 709/229; 709/217, 709/219, 709/223, 709/224, 713/155, 717/172, 717/177, 726/3

FIELD-OF-SEARCH: 709/229, 709/217, 709/232, 709/224, 709/226, 709/230, 709/223, 709/225, 709/200, 709/201, 709/202, 709/203, 709/219, 713/155, 713/200, 713/201, 717/172, 717/177, 717/178

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
5919247	July 1999	Van Hoff et al.	709/217
5974549	October 1999	Golan	713/200
6088803	July 2000	Tso et al.	713/201
6154844	November 2000	Touboul et al.	713/201
6158010	December 2000	Moriconi et al.	709/223
6233341	May 2001	Riggins	380/277

6301661	October 2001	Shambroom	713/168
6367012	April 2002	Atkinson et al.	713/176
6473800	October 2002	Jerger et al.	709/226
6499109	December 2002	Balasubramaniam et al.	713/201

ART-UNIT: 2153

PRIMARY-EXAMINER: Jean; Frantz B.

ASSISTANT-EXAMINER: Choudhary; Anita

ATTY-AGENT-FIRM: Keohane; Stephen T. Beckstrand; Shelley M.

ABSTRACT:

A workflow, enterprise, and mail-enabled application server and platform supports distributed computing and remote execution of web applications. Lotus Domino Offline Services (DOLS) is used by a web site administrator to configure Internet Notes (iNotes) clients to auto download from server, thus providing iNotes clients with web access using HTTP with various browsers, and with local processing and replication. A local run time model comprises a hierarchy of models including object data store model, security model, indexing model, replication model, agent workflow model and mail model. DOLS provides a layered security model that allows flexibility for controlling access to all or part of an application. The highest level of security is managed through a database access control list (ACL). Further refinements within the security model provide access to specific documents, and their views, forms or folders, and include read access lists, write access lists, form access lists and readers and authors fields.

19 Claims, 26 Drawing figures

☐ 128. Document ID: US 6845383 B1

L19: Entry 128 of 160 File: USPT Jan 18, 2005

US-PAT-NO: 6845383
DOCUMENT-IDENTIFIER: US 6845383 B1

TITLE: System and method for managing concurrent scheduled or on-demand replication of subscriptions

DATE-ISSUED: January 18, 2005

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Kraenzel; Carl J.	Boston	MA		
Immerman; John D.	Sudbury	MA		
Mills; William A.	Arlington	MA		
Nowacki; Mark A.	Wilmington	MA		
Lu; Jeannie J.	West Roxbury	MA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
International Business Machines Corporation	Armonk	NY			02

APPL-NO: 09/ 596783 [PALM]
DATE FILED: June 19, 2000

PARENT-CASE:
CROSS REFERENCES TO RELATED APPLICATIONS The following U.S. patent applications filed concurrently herewith are assigned to the same assignee hereof, contain subject matter related, in certain respect, to the subject matter of the present application and are incorporated herein by reference: U.S. patent application Ser. No. 09/596,283 filed 19 Jun. 2000 for "System and Method for Providing a Distributable Runtime"; U.S. patent application Ser. No. 09/596,282 filed 19 Jun. 2000 for "System and Method for Downloading Security Context Elements Governing Execution of Downloadable and Distributable Agents"; U.S. patent application Ser. No. 09/596,963 filed 19 Jun. 2000 for "System and Method for Selective Replication of Databases Within a Workflow, Enterprise, and Mail-Enabled Web Application Server and Platform"; U.S. patent application Ser. No. 09/597,997 filed 19 Jun. 2000 for "System and Method For Providing a Distributable Runtime That Deploys Web Applications and Services From a Workflow, Enterprise, and Mail-Enabled Web Application Server and Platform"; U.S. patent application Ser. No. 09/596,745 filed 19 Jun. 2000 for "A System and Method for a Web Based Trust Model Governing Delivery of Services and Programs"; and U.S. patent application Ser. No. 09/596,845 filed 16 Jun. 2000 for "A System and Method for Developing and Administering Web Applications and Services From a Workflow, Enterprise, and Mail-Enabled Web Application Server and Platform.

INT-CL: [07] G06 F 17/30

US-CL-ISSUED: 707/200; 707/9, 707/8
US-CL-CURRENT: 707/200; 707/8, 707/9

FIELD-OF-SEARCH: 707/1-10, 707/100-205, 709/218

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
6256670	July 2001	Davies	709/224
6259405	July 2001	Stewart et al.	342/457
6272537	August 2001	Kekic et al.	709/223
6292790	September 2001	Krahn et al.	700/79
6295482	September 2001	Tognazzini	700/231
6381742	April 2002	Forbes et al.	717/11
6393468	May 2002	McGee	707/513
6421714	July 2002	Rai et al.	709/217
6446092	September 2002	Sutter	707/203
6453353	September 2002	Win et al.	709/225

ART-UNIT: 2177

PRIMARY-EXAMINER: Robinson; Greta

ASSISTANT-EXAMINER: Pannala; Sathyanarayan

ATTY-AGENT-FIRM: Keohane; Stephen T. Beckstrand; Shelley M.

ABSTRACT:

A workflow, enterprise, and mail-enabled application server and platform supports distributed computing and remote execution of web applications. Lotus Domino online services (DOLS) is used

by a web site administrator to configure Internet Notes (iNotes) clients to auto download from server, thus providing iNotes clients with web access using HTTP with various browsers, and with local processing and replication. A local run time model comprises a hierarchy of models including object data store model, security model, indexing model, replication model, agent workflow model and mail model. DOLS provides a layered security model that allows flexibility for controlling access to all or part of an application. The highest level of security is managed through a database access control list (ACL). Further refinements within the security model provide access to specific documents, and their views, forms or folders, and include read access lists, write access lists, form access lists and readers and authors fields.

22 Claims, 26 Drawing figures

☐ 129. Document ID: US 6785721 B1

L19: Entry 129 of 160 File: USPT Aug 31, 2004

US-PAT-NO: 6785721
DOCUMENT-IDENTIFIER: US 6785721 B1

TITLE: System and method for providing a distributable runtime that deploys web applications and services from a workflow, enterprise, and mail-enabled web application server and platform

DATE-ISSUED: August 31, 2004

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Immerman; John D.	Sudbury	MA		
Kraenzel; Carl J.	Boston	MA		
Mills; William A.	Arlington	MA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
International Business Machines Corporation	Armonk	NY			02

APPL-NO: 09/ 597997 [PALM]
DATE FILED: June 19, 2000

PARENT-CASE:
CROSS REFERENCE TO RELATED APPLICATIONS The following U.S. patent applications filed concurrently herewith are assigned to the same assignee hereof, contain subject matter related, in certain respect, to the subject matter of the present application and are incorporated herein by reference: U.S. patent application Ser. No. 09/596,283 for "System and Method for Providing a Distributable Runtime"; U.S. patent application Ser. No. 09/596,282 for "System and Method for Downloading Security Context Elements Governing Execution of Downloadable and Distributable Agents"; U.S. patent application Ser. No. 09/596,963 for "System and Method for Selective Replication of Databases Within a Workflow, Enterprise, and Mail-Enabled Web Application Server and Platform"; U.S. patent application Ser. No. 09/596,783 for "System and Method for Managing Concurrent Scheduled or On-demand Replication of Subscriptions"; U.S. patent application Ser. No. 09/596,745 for "A System and Method for a Web Based Trust Model Governing Delivery of Services and Programs" and U.S. patent application Ser. No. 09/596,845 for "A System and Method for Developing and Administering Web Applications and Services From a Workflow, Enterprise, and Mail-Enabled Web Application Server and Platform

INT-CL: [07] G06 F 15/16

US-CL-ISSUED: 709/220; 709/221

US-CL-CURRENT: 709/220; 709/221

FIELD-OF-SEARCH: 709/220, 709/221, 709/217, 709/218, 709/203, 709/250, 709/226, 717/172, 717/171

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
5455903	October 1995	Jolissaint et al.	345/835
6226623	May 2001	Schein et al.	705/35
6269394	July 2001	Kenner et al.	709/217
6381742	April 2002	Forbes et al.	717/176
6393468	May 2002	McGee	709/218

ART-UNIT: 2157

PRIMARY-EXAMINER: Maung; Zarni

ASSISTANT-EXAMINER: Halim; Sahera

ATTY-AGENT-FIRM: Keohane; Stephen T. Bekcstrand; Shelley M.

ABSTRACT:

A workflow, enterprise, and mail-enabled application server and platform supports distributed computing and remote execution of web applications. Lotus Domino online services (DOLS) is used by a web site administrator to configure Internet Notes (iNotes) clients to auto download from server, thus providing iNotes clients with web access using HTTP with various browsers, and with local processing and replication. A local run time model comprises a hierarchy of models including object data store model, security model, indexing model, replication model, agent workflow model and mail model. DOLS provides a layered security model that allows flexibility for controlling access to all or part of an application. The highest level of security is managed through a database access control list (ACL). Further refinements within the security model provide access to specific documents, and their views, forms or folders, and include read access lists, write access lists, form access lists and readers and authors fields.

18 Claims, 26 Drawing figures

☐ 130. Document ID: US 6772157 B2

L19: Entry 130 of 160 File: USPT Aug 3, 2004

US-PAT-NO: 6772157
DOCUMENT-IDENTIFIER: US 6772157 B2

TITLE: Delegated administration of information in a database directory

DATE-ISSUED: August 3, 2004

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY

Barnett; Janet Arlie	Pattersonville	NY
Vivier; Barbara Jean	Niskayuna	NY
Aggour; Kareem Sherif	Schenectady	NY
Kornfein; Mark Mitchell	Latham	NY

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
General Electric Company	Niskayuna	NY			02

APPL-NO: 09/ 761000 [PALM]
DATE FILED: January 16, 2001

PARENT-CASE:
CROSS REFERENCE TO RELATED APPLICATIONS This application claims the benefit of U.S. Provisional Application Serial No. 60/241,645 filed on Oct. 19, 2000, and entitled "Approach And Design For Software To Facilitate Delegated Administration Of Information In A Database Directory," which is incorporated by reference herein in its entirety.

INT-CL: [07] G06 F 17/30

US-CL-ISSUED: 707/9; 707/10, 709/206, 709/229, 709/246, 713/201
US-CL-CURRENT: 707/9; 707/10, 709/206, 709/229, 709/246, 726/1, 726/3

FIELD-OF-SEARCH: 707/10, 707/3, 707/101, 707/9, 707/103, 709/217, 709/218, 709/227, 709/229, 709/206, 709/246, 713/201

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
5671360	September 1997	Hambrick et al.	705/9
6073242	June 2000	Hardy et al.	713/201
6088451	July 2000	He et al.	
6144959	November 2000	Anderson et al.	
6408336	June 2002	Schneider et al.	709/229

OTHER PUBLICATIONS

Oblix NetPoint 4.0 [online]. Oblix, Inc. [retrieved on Dec. 18, 2000]. Retrieved from the Internet:<URL: http://www.oblix.com/products_and_solutions/netpoint/>.
Securant Products [online]. Securant Technologies [retrieved on Dec. 18, 2000]. Retrieved from the Internet: <URL: http://www.securant.com/ie/main_products.html>.
Delegated Management Services [online]. Netegrity, Inc. [retrieved on Dec. 18, 2000]. Retrieved from the Internet: <URL: http://www.netegrity.com/products/dms.html>.
iPlanet Delegated Administrator 4.5 Datasheet [online]. iPlanet International [retrieved on Dec. 18, 2000]. Retrieved from the Internet:<URL: http://iplanet.com/products/infrastructure/dir_security/del_admin/>.

ART-UNIT: 2172

PRIMARY-EXAMINER: Corrielus; Jean M.

ATTY-AGENT-FIRM: Goldman; David C. Patonode; Patrick K.

ABSTRACT:

A delegated administration tool for administrating information in a database directory. The delegated administration tool enables an administrator to delegate administration and various types of administrative authority to other users within a community of users. In particular, an administrator with proper authority may create new administrative domains and assign authority referred to as delegation authority and edit authority to other users. The creation of additional administrative domains and the assignment of the delegation authority and edit authority can continue to an arbitrary level within the community.

48 Claims, 17 Drawing figures

Terms	Documents
L18 and (admin or administrative) with domain	160

L18: Entry 782 of 910 File: USPT Feb 20, 2001

US-PAT-NO: 6192405
DOCUMENT-IDENTIFIER: US 6192405 B1

TITLE: Method and apparatus for acquiring authorized access to resources in a distributed system

DATE-ISSUED: February 20, 2001

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Bunnell; Karl Lee	American Fork	UT		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Novell, Inc.	Provo	UT			02

APPL-NO: 09/ 012506 [PALM]
DATE FILED: January 23, 1998

INT-CL: [07] G06 F 13/00

US-CL-ISSUED: 709/225; 709/202, 709/219, 709/313
US-CL-CURRENT: 709/225; 709/202, 709/219, 719/313

FIELD-OF-SEARCH: 709/201, 709/202, 709/217, 709/206, 709/219, 709/223, 709/225, 709/224, 709/313, 709/315, 709/328, 709/329, 709/330, 707/10, 707/100, 707/103, 707/104, 707/501

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5603031	February 1997	White et al.	
☐	5649194	July 1997	Miller et al.	707/200
☐	5913025	June 1999	Higley et al.	707/9
☐	5922074	July 1999	Richard et al.	713/200
☐	5933826	August 1999	Ferguson	707/9
☐	5944824	August 1999	He	713/201
☐	6014686	January 2000	Elnozahy et al.	709/202

OTHER PUBLICATIONS

Novell, Inc. Novell Improves Decision-Making, Responsiveness and Competitiveness for Networked

Enterprises., Jul. 30, 1997.
Novell, Inc. Novell's Guide to NetWare 4.1 Networks, Table of Contents and Chapters 3 and 13, J. Hughes et al. 1996.
Informs-Electronic Forms Automation V 4.1-Designer, Table of Contents, Chapter 13, Appendices D & I, 1995.

ART-UNIT: 214

PRIMARY-EXAMINER: Vu; Viet D.

ATTY-AGENT-FIRM: Dinsmore & Shohl LLP

ABSTRACT:

A computer system has a management service, such as a distributed directory, having a plurality of objects and an access control mechanism. The computer system also has a resource, such as a data store, with a security system. A first object in the management service represents a requester and a second object represents the resource. A broker has access to the management service and the resource, and is operative to determine whether the first object has rights to access the second object, and if such rights exist, allow the requester to access the resource.

22 Claims, 9 Drawing figures

Previous Doc Next Doc Go to Doc#

L18: Entry 782 of 910 File: USPT Feb 20, 2001

DOCUMENT-IDENTIFIER: US 6192405 B1
TITLE: Method and apparatus for acquiring authorized access to resources in a distributed system

Drawing Description Text (8):
FIG. 6 depicts a computer system and the interrelationship between a user, and e-mail system acting as a broker, a distributed directory, a database, and an administrator program;

Detailed Description Text (6):
When a group of computers are connected to one another, such as in a client/server network, a management service is typically used to organize, administer, and provide access to information and resources across the network. Management services usually access or include a collection of objects that represent a variety of things. For instance, some typical objects represent users, groups, printers, computers, and the like. In some management services, objects are organized in flat domains such as the SECURITY ACCOUNTS MANAGER ("SAM") of WINDOWS NT.

Detailed Description Text (22):
Directory security is usually used in conjunction with login security, where directory security is not used unless login security has been first verified. While directory security can vary greatly, it generally comprises two parts: file system security and object security. File system security provides access control to files and directories, and basically involves assigning trustee rights and file/directory attributes. Trustee rights assignments can be granted to any object in the distributed directory including container objects, user objects, group objects, and organization roles. Examples of such rights include access control, supervisor, read, write, create, erase, modify, and file scan. In contrast, file/directory attributes control what actions can or cannot be taken on a file or directory. For example, certain files could be flagged as "read only" and "shareable" to prevent any unintentional or intentional deletions of such files or directories.

Detailed Description Text (58):
In addition to these new object classes, the administrator 107 also extends the following existing object classes: (i) User, (ii) Group, (iii) Organization, (iv) Organizational Unit, and (v) Country.

Detailed Description Text (75):
These modifications allow forms to be associated with an specific "User" object, "Group", "Organization", "Organizational Unit" or "Country". The administrator 107, in addition to allowing these associations to be configured for each of these objects, also creates an ACL on the Forms object 104 with the "Read" right to all attributes for each association made to a Forms object 104.

Detailed Description Text (100):
In step 165, the Forms Processor Client 113 is in "Service" mode and waits for an appropriate command. When the "Form Request" dialog is invoked in step 166, the Forms Processor Client 113 presents the user 108 with a list of all available forms on the "Form Request" dialog. This involves reading the current authenticated NDS object 102 "Forms" attribute, reading the "Forms" attribute of all the NDS groups the current user is a member, reading each container above the current authenticated object up to the [Root], and place all values in an internal object list. At step 168, the user 108 simply double-clicks the form of interest on the list and the request is submitted in step 169 to the Forms Processor Server 112. The Forms Processor Server 112 processes the request and responds with a custom message type, as discussed above.

Detailed Description Text (102):

The computer system 100 provides the capability for NDS/GROUPWISE clients to request and submit data from a database 109 while leveraging NDS authentication and using the secure transport of GROUPWISE. A GROUPWISE client with the Forms Processor Client 113 loaded can request to request a form by clicking on the Request Form tool bar button. This launches the Request Form dialog box. Enumerated on this dialog box are the Form objects 104 the user 108 has been granted rights to request. This is accomplished by reading the Form associations from the current authenticated user object 102, the groups this user is member of, and each of the containers above this user object up to [Root]. The user 108 can then request one of the enumerated forms from that dialog.

Previous Doc Next Doc Go to Doc#

L18: Entry 807 of 910 File: USPT Apr 11, 2000

US-PAT-NO: 6049799
DOCUMENT-IDENTIFIER: US 6049799 A

TITLE: Document link management using directory services

DATE-ISSUED: April 11, 2000

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Mangat; Satwinder S.	Orem	UT		
Taylor; Wayne	Provo	UT		
Mahlum; Steven	Orem	UT		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Novell, Inc.	Provo	UT			02

APPL-NO: 08/ 854391 [PALM]
DATE FILED: May 12, 1997

INT-CL: [07] G06 F 17/30

US-CL-ISSUED: 707/10; 707/1, 707/2, 707/201, 709/203, 709/221, 710/11, 714/15, 370/396
US-CL-CURRENT: 707/10; 370/396, 707/1, 707/2, 707/201, 709/203, 709/221, 710/11, 714/15

FIELD-OF-SEARCH: 707/1, 707/2, 707/8, 707/9, 707/10, 707/200, 707/202, 707/203, 707/204, 707/100, 707/201, 707/3, 707/4, 707/513, 707/501, 710/11, 395/187.01, 395/200.53, 395/200.03, 709/203, 709/221, 714/15, 370/396

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4899299	February 1990	Macphail	707/204
☐	5497463	March 1996	Stein et al.	395/200.03
☐	5504891	April 1996	Motoyama et al.	707/513
☐	5548726	August 1996	Pettus	709/221
☐	5594921	January 1997	Pettus	710/11
☐	5717922	February 1998	Hohensee et al.	707/100
☐	5761683	June 1998	Logan et al.	707/513
☐	5778385	July 1998	Pratt	707/200

☐	5787442	July 1998	Hacherl et al.	707/201
☐	5794232	August 1998	Mahlum et al.	707/3
☐	5825772	October 1998	Dobbins et al.	370/396
☐	5828833	October 1998	Belville et al.	395/187.01
☐	5832225	November 1998	Hacherl et al.	395/200.53
☐	5835698	November 1998	Harris et al.	714/15
☐	5850518	December 1998	Northrup	709/203
☐	5887171	March 1999	Tada et al.	707/4
☐	5893122	April 1999	Tabuchi	707/501
☐	5987471	November 1999	Bodine et al.	707/103

ART-UNIT: 271

PRIMARY-EXAMINER: Black; Thomas G.

ASSISTANT-EXAMINER: Rones; Charles L.

ATTY-AGENT-FIRM: Madson & Metcalf

ABSTRACT:

The present invention provides a method and apparatus for managing links between documents and other data structures, such as applications. Search mechanisms may include a directory services search engine for locating objects. A directory object data structure search engine may evaluate, search, or the like, various objects to obtain important information contained in attributes or data members thereof. An association list handler may be a search engine for searching association lists stored as attributes of objects for identifying desired documents. A standard query data structure may be applied by a query resolver to a document location table identified by a document location object. A query generator may be responsible to formulate the standard query data structure, or for formulating queries for all three types of search engines. A directory services database may be searched for an object. An object may be searched for a particular data member or attribute. A table may be pointed to by a directory services object. The table may be searched for an identification or distinguished name associated with a specific document desired. Likewise, fuzzy logic may be applied to obtain documents that are similar to desired documents that are similar to desired documents, rather than identical.

33 Claims, 14 Drawing figures

Previous Doc Next Doc Go to Doc#

L18: Entry 807 of 910 File: USPT Apr 11, 2000

DOCUMENT-IDENTIFIER: US 6049799 A
TITLE: Document link management using directory services

Brief Summary Text (12):
It is an object of the invention to provide a new type of directory services object that may be used to provide document management of documents accessed by users, groups of users, organizations, and the like.

Detailed Description Text (47):
For example, the add executable 106 may include a test beginning at a closest proximity to a user or an application 74. Accordingly, criteria may include a test to identify a user identified in an access list, or search lists of a user's membership in a particular group or organization. Tests may evaluate contents, titles, or paths similar to those of a desired document. Such information may help determine that a high probability exists for a document 144 to be included for consideration by a user, if an exact match is not found.

Detailed Description Text (62):
A leaf object, such as a user object 128, Docloc object 130, or group object 120 does not contain other objects. A group object 120 identifies members of a group. Thus, a group object 120 may include certain rights 122 and similar attributes. However, a significant feature of a group object 120 is a membership list 124. Typically, a membership list 124 may contain a list of distinguished names 126. Distinguished names are unique names identifying member objects 113 that pertain to a group 120 defined by the group object 120.

Detailed Description Text (95):
Alternatively, one may think of the individual distinguished names 198 contained in a membership list 124 as individual attributes as well. The distinguished names 198 may identify users, for example, or user objects 128 having some relationship to the group object 120. A group object 120 may be thought of as defining a group 120.

Detailed Description Text (101):
Querying responsibilities may be allocated to the directory services search engine 138 to find a Docloc object 130, 132, a user object 128, a group object 120, or a container object 114. Meanwhile, responsibility may be placed upon the association list handler 88, in conjunction with, or independently of, the directory services search engine 138 to query association lists 118, 136, 200 to identify objects 113 identified therein by respective distinguished names 160, 180, 210, and the like. Meanwhile the query resolver 84 may be allocated the single responsibility of querying or resolving a query directed to a Docloc table 140, a Docloc object 130, or the like.

Detailed Description Text (158):
Failing to find the desired document 144 by looping 330 through all Docloc objects 130 identified in or by the user object 128, the loop step 330 may loop outward through group objects 120 related to the user object 128. Again, the nested looping 330 continues through the Docloc objects 130 referenced by the group object 120.

Detailed Description Text (160):
Similarly, all container objects 114, which may be thought of as parent objects 114 to user objects 128 or even group objects 120, may be looped through 330, in turn. An objective of a loop step 330 is to loop through each type of object 113 (e.g. Docloc objects 130, user objects 128, group objects 120, container objects 118) in order to identify a desired Docloc object 130.

Detailed Description Text (162):
Each time a loop step 330 loops through a particular type of object 113 (e.g. container object 114, group object 120, user object 128, Docloc object 130), it should ultimately arrive at a Docloc object 130, if available. A query data structure 80, or query 80, in combination with a query resolver 84 (see FIG. 2) may then evaluate the attributes 214 of the Docloc object 130, and vector to a Docloc table 140. Likewise, a query 80 or standard query data structure 80 in combination with a query resolver 84 (distinct from such for querying a Docloc object 130) may query a Docloc table 140 to find a file name 280 and path 282 corresponding to a desired document 144. Thus, in FIG. 11 the resolve query step 334 may be thought of as querying a Docloc table 140 to find an appropriate file name 280 and path 282 corresponding to a desired document 144.

Detailed Description Text (166):
After a resolve query step 334, a test 340 may determine whether or not an exact match for a desired document 144 has been located in a Docloc table 140. If not, a test 342 may determine whether or not the traverses of all suitable objects 113 (e.g. Docloc objects 130, 132, user objects 128, group objects 120, and container objects 114 or parent objects 114) have been exhausted. If not, the nested, looping step 330 continues. If the traverse is complete, or an exact match was found, the process 320 advances.

Detailed Description Text (183):
In general, the provide distinguished name step 366 may be thought of as providing a particular distinguished name corresponding to any type of object 213. For example, a Docloc object 130, 132, a user object 128, a group object 120, or a container object 114 may be thought of as a "type" or class of object 113 in a directory services database 112.

Detailed Description Text (184):
A nested looping may traverse through all Docloc objects 130, 132, followed by user objects 128, followed by group objects 120, and container objects 114 (parent objects 114). The looping may rely on a provide step 366 providing a next distinguished name of the appropriate type of object 113. Thus, the provide step 366 may initially provide a distinguished name 213 corresponding to a Docloc object 130, 132.

Detailed Description Text (186):
A search step 370 may be responsible for searching through one or more directory services databases 112 to find the desired type of object 113 (e.g. Docloc objects 130, 132, user object 128, group object 120, container object 114) in question. In one presently preferred embodiment, the search step 370 searches for a distinguished name 213, 170, 190, 150, as appropriate. In one embodiment, the directory services search engine 138 may execute the search step 370.

Detailed Description Text (202):
The find step 390 and the provide step 366, combine to step through each of the distinguished names 160, 180, 210 in the respective association lists 118, 136, 200 as the process 350 loops through each of the respective objects 114, 128, 120. In one currently preferred embodiment, as discussed, the process 350 loops in a nested fashion first through Docloc objects 130, then user objects 128, then group objects 120, then container objects 114 (parent objects 114).

CLAIMS:

5. A method for managing a link to a document, the method comprising:

providing a network directory services system for storing and managing a directory services database of directory services objects, including a document location object, being an instance of a directory services object, linked together in a hierarchy over a network;

providing a link management module for reestablishing a link to a lost document by searching through multiple environments across the network to find the location of the lost document, the link management module being independent from the directory services system and programmed to query the directory services system to find the document location object corresponding to the lost document;

providing a file server storing a plurality of documents, including the lost document;

detecting a link failure;

generating a query containing information corresponding to the link failure;

traversing, by the link management module, the directory services database to locate the document location object corresponding to the document;

reestablishing, by the link management module, the link.

15. A method for managing a link to a document, the method comprising:

providing a network directory services system for storing and managing a directory services database of directory services objects, including a document location object, being an instance of a directory services object, linked together in a hierarchy over a network of nodes, each node containing a processor effective to execute executables;

executing an installation utility programmed to install the document on a node, the installation utility being independent from the directory services system;

providing information effective to locate the document; and

storing to the document location object in the directory services database attributes reflecting the information.

20. An apparatus for managing links to documents within a network of nodes, the nodes including a user station, file server, and directory services server, the apparatus comprising:

the user station programmed to execute a link management module for searching through multiple environments across the network to find and link a lost document to the user station;

a file server storing a plurality of documents, including the lost document;

a directory services system comprising a directory services database, containing directory services objects, including a document location object, being an instance of a directory services object, linked together in a hierarchy, and programmed to execute a search engine effective to search the directory services database for the directory services objects associated with the lost document

the link management module being independent from the directory services system and programmed to query the directory services system to find the document location object corresponding to the lost document.

23. The apparatus of claim 22, wherein the directory services database stores objects selected from the document location object, a user object, group object, and container object, the document location object being comparatively closest to the link and containing pointing data for identifying the document.

Previous Doc Next Doc Go to Doc#

L16: Entry 16 of 17 File: USPT Oct 1, 2002

US-PAT-NO: 6460141
DOCUMENT-IDENTIFIER: US 6460141 B1

TITLE: Security and access management system for web-enabled and non-web-enabled applications and content on a computer network

DATE-ISSUED: October 1, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Olden; Eric M.	San Francisco	CA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
RSA Security Inc.	Bedford	MA			02

APPL-NO: 09/ 182265 [PALM]
DATE FILED: October 28, 1998

INT-CL: [07] G06 F 12/14

US-CL-ISSUED: 713/201; 713/202
US-CL-CURRENT: 726/4; 726/12, 726/13, 726/14

FIELD-OF-SEARCH: 713/200, 713/201, 713/202, 713/203

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5557747	September 1996	Rogers et al.	395/200.11
☐	5968176	October 1999	Nessett et al.	713/201
☐	5983270	November 1999	Abraham et al.	709/224
☐	5983350	November 1999	Minear et al.	713/201
☐	6088451	July 2000	He	380/25
☐	6151606	November 2000	Mendez	707/201
☐	6158010	December 2000	Moriconi et al.	713/201
☐	6205415	March 2001	Butts et al.	703/27
☐	6233542	May 2001	Butts et al.	703/27
☐	6233543	May 2001	Butts et al.	703/27

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
WO 00/25214	May 2000	WO	

OTHER PUBLICATIONS

U.S. application No. 09/483,645, Field et al., filed Jan. 14, 2000.
User Guide for Bankers Trust, Authorization Manager, Aug. 13, 1997.
User Guide for Bankers Trust, Security Instructions Services, Oct. 1, 1997.

ART-UNIT: 2131

PRIMARY-EXAMINER: Wright; Norman M.

ATTY-AGENT-FIRM: Testa, Hurwitz & Thibeault, LLP

ABSTRACT:

A security and access management system provides unified access management to address the specific problems facing the deployment of security for the Web and non-Web environment. Unified access management consists of strategic approaches to unify all key aspects of Web and non-Web security policies, including access control, authorization, authentication, auditing, data privacy, administration, and business rules. Unified access management also addresses technical scalability requirements needed to successfully deploy a reliable unified Web and non-Web security system. The security and access management system provides the technology required to support these key factors as they relate to Web and non-Web security. The security and access management system operates in combination with network and system security tools such as firewalls, network intrusion detection tools, and systems management tools to provide comprehensive security for the Web-enabled enterprise.

3 Claims, 37 Drawing figures

Previous Doc Next Doc Go to Doc#

L16: Entry 16 of 17 File: USPT Oct 1, 2002

DOCUMENT-IDENTIFIER: US 6460141 B1
TITLE: Security and access management system for web-enabled and non-web-enabled applications and content on a computer network

Detailed Description Text (20):
The security and access management system 10 provides a highly flexible and scalable data model for defining both accessibility of resources and applications and data model administration policy. While the security and access management system 10 provides out-of-the-box support for Web-based applications, the security and access management system is also powerful and flexible enough to secure proprietary applications, such as the applications which run on the non-Web server 30 shown in FIG. 1. Security policy is defined using an access control architecture. Through the access control architecture, protected resources are associated with resource consumers, defining access control policy. Additionally, the security and access management system 10 provides a robust administration architecture, securing access to the entitlements database 32. Through the administration architecture, a user is associated with administrative rights and ownership, defining an administrative policy.

Detailed Description Text (25):
The resource consumer architecture 56 also provides a containment hierarchy or containers 74 of users 68. This allows an administrator to more easily assign access rights to a large group of users 68 without having to assign rights individually. A user 68 can be grouped together into a group object 76. Group objects 76 likewise can be grouped together into a realm object 78.

Detailed Description Text (46):
User means a single user of Web applications protected by the security and access management system 10, using various user properties such as username, password, e-mail address, IP address, etc. Group means a collection of users, grouped together for ease of administration. Groups have specific properties. A realm is a collection of groups. A realm contains all of the users within the component groups of the realm. Entity means a user, group, or realm.

Detailed Description Text (49):
An administrative group is a set of ownable resources that is configured to be under the control of a particular set of administrators. Administrative role means a role defining the types of operations an administrator can perform on a particular administrative group. An ownable resource is one of all of the types of resources defined in the security and access management system 10, which can fall under the control of an administrative group. They are: user, group, realm, application, Web server, administrative roles, and user property definitions. Other resources, such as entitlements and smart rules, are owned by default by the group that owns the related application, property, or user/group/realm.

Detailed Description Text (50):
As mentioned earlier, the security and access management system 10 encompasses various concepts. These concepts include users, groups, and realms.

Detailed Description Text (52):
A group is a collection of users. Any action applied to a group is automatically applied to every user in that group. Consequently, granting a group access to an application automatically gives each user in that group access to that application. The same rule applies for restricting application access and various other features. The exception to this rule is deleting a group. If a group is deleted, the users in that group are no longer members of that group, and none of the security settings applied to that group continues to apply to those users. However, deleting a group does not delete any of the users in that group. Users must be deleted individually to remove their information from the entitlements database 32 and make them

unavailable to the administrator.

Detailed Description Text (58):
As shown in FIG. 5, a user can be associated with any number of administrative roles. An administrative role can be associated with any number of users. An administrative group can contain any number of users, groups, or realms.

Detailed Description Text (66):
The security and access management system 10 allows a security administrator to create an unlimited number of users, each with individual defining properties. The administrator can further collect users into groups and groups into realms. Additionally, users can be in multiple groups. This feature is useful for administrators trying to mimic organizational structure (for example, user John Doe may be in the promotions group, which is in the marketing realm) or geography (user Jane Doe is in the Paris group, which is in the Europe realm), or any other type of grouping. The user/group/realm concept is also important for setting permissions and entitlements, as will be described later in connection with the description of the Basic Entitlements page.

Detailed Description Text (67):
In order to find a particular user, group, or realm in the list box, an administrator can scroll through the list of entities or use the Search function. In order to use Search, the administrator enters the desired name or name fragment in the field, and clicks the Search button. If a full name is typed into the Search field, that name will automatically appear at the top of the list box. If a fragment is typed into the Search field, the first name beginning with that fragment will appear at the top of the list box. The Search function is indexed differently depending on the type of entity selected. For users, the Search function indexes on last name. For groups and realms, the Search function indexes on the group or realm name.

Detailed Description Text (68):
Users logged in using administrative roles with the proper permissions can create users, groups, or realms. In order to create a user, Users is selected in the entity menu. Clicking the Create button brings up the Create User dialog window, as shown in FIG. 9.

Detailed Description Text (73):
The Create User window also comprises a Super User checkbox. A user must be an administrator to be designated a Super User. If a user is both an administrator and a Super User, he or she can perform any action on any user, group, realm, or application. Care is typically exercised when applying Super User status to administrators.

Detailed Description Text (78):
When creating a user, group, or realm, an administrator should be aware of his or her current administrative role and the administrative group associated with that role. Any user, group, or realm created is automatically associated with that administrative group. Consequently, if an administrator can create users as both the marketing administrator and the engineering administrator, for example, it is preferable to create marketing and engineering users while working in the appropriate roles.

Detailed Description Text (80):
On the one hand, in order to add users to a group, Users is selected in the entity menu. The user list appears in the entity list box. Then, the Select Group button is clicked. The Group List dialog window will appear. The group to be populated is then selected, and the OK button is clicked. In order to include users in that group, the user to be added is highlighted to select the user, and the Add Arrow button is then clicked.

Detailed Description Text (81):
On the other hand, in order to remove users from a group, Users is selected in the entity menu, and the appropriate group is also selected, as described above. The user to be removed is then highlighted to select the user from the Group Members list box. In order to remove the selected user, the Remove Arrow button is then clicked.

Detailed Description Text (83):
In order to edit a user, group, or realm, Users, Groups, or Realms is selected from the entity menu. All of the available entities of that type then appear in the list box below. The user, group, or realm to be modified is then highlighted to select the entity, and then the Modify

button is clicked. The Modify dialog window appears. The Modify dialog window is identical to the Create dialog window, but contains all of the current user/group/realm information, which can be edited. Once the fields in the Modify dialog window have been changed, OK is clicked to complete the Modify, or the Cancel button is clicked to abort.

Detailed Description Text (84):
In order to delete an entity, the appropriate entity type (Users, Groups, or Realms) from the entity menu is selected. Then, the entity or entities to be deleted from the list box are highlighted. The Delete button is pressed to delete the user, group, or realm.

Detailed Description Text (85):
Deleting a group or user is different from removing a group from a realm, or a user from a group. A deleted group is gone. The component users still exist, but the group information is deleted, and any entitlements applied to that group are deleted as well, and the group is automatically deleted from any realm which contained that group. A group removed from a realm still exists. However, the group is simply no longer governed by entitlements applied to that realm. Similarly, a deleted user is gone. All of the user information is removed from the entitlements database 32. Deleting a user automatically removes that user from all groups, and a deleted user cannot be added to any group. A removed user is no longer a member of that group, but is still in the entitlements database 32 and is available to be added to any group. Consequently, care is typically exercised when deleting users, groups, or realms.

Detailed Description Text (96):
Entitlements are defined and administered using the Basic Entitlements page, as shown in FIG. 17. By adding entitlements using the security and access management system 10, entitlements to particular applications can be assigned to users, groups, or realms with ease. First, the administrator selects the user, group, or realm to be granted the entitlement. This is similar to the selection process on the Users page, described earlier. The appropriate entity is then selected from the entity menu. Clicking the left Choose button brings up a list of all available users, groups, or realms. The entity to be administered is selected from this list, and the Choose button is clicked. All of the entitlements for the selected user, group, or realm appear in the Basic Entitlements list box.

Detailed Description Text (98):
In order to grant a Basic Entitlement to the selected user, group, or realm, the appropriate application function is highlighted, and the Left Arrow button is clicked. The application name, function name, and default entitlement setting (Allow or Deny) will then appear in the Basic Entitlements list box for the user.

Detailed Description Text (101):
If a basic entitlement for a user is deleted, the access privileges of that user to that application function revert to the next available setting. If the user is in a group or realm with basic entitlements set for that application function, those privileges apply. If that is not the case, default settings apply.

Detailed Description Text (102):
When a basic entitlement for a group is deleted, users in that group, who do not have basic entitlements set, revert to the default entitlement settings for that application function. Since entitlements at the user level override entitlements at the group level, users with basic entitlements set see no change in their access ability.

Detailed Description Text (103):
When basic entitlements for a realm are deleted, access privileges for users in groups in that realm are determined by the appropriate user entitlements settings (if they exist), group entitlements settings (if they exist), or default entitlements settings, in that order.

Detailed Description Text (125):
Referring to FIG. 23, the Administrators page is the tool for defining security administrators and administrative duties. An administrator can be given the power to control any selection of users, groups, or realms, any applications, and any privileges. The design of the administrative system will now be described in more detail.

Detailed Description Text (197):
The security and access management system 10 can leverage data that resides in an LDAP

directory like other LDAP-enabled applications. By leveraging the LDAP directory data, organizations can centrally manage user information in the directory and use the security and access management system 10 to define security policy and to secure Web resources.

Detailed Description Text (198):
In a preferred embodiment, the security and access management system 10 provides a Web security system that combines native LDAP support with powerful Oracle database scalability. This combination of the security and access management system 10 and LDAP provides many benefits and enables: 1) companies to use an LDAP directory server to centrally store and manage user information, such as passwords, e-mail addresses, contract numbers, and other common user attributes; 2) companies to use multiple LDAP directory servers, including those from Netscape or Novell; 3) Web applications to incorporate users' LDAP attributes to dynamically generate personalized Web pages; and 4) Business to business application and data integration across firewalls via LDAP.

Previous Doc Next Doc Go to Doc#

L16: Entry 8 of 17 File: USPT Apr 6, 2004

US-PAT-NO: 6718535
DOCUMENT-IDENTIFIER: US 6718535 B1
**** See image for Certificate of Correction ****

TITLE: System, method and article of manufacture for an activity framework design in an e-commerce based environment

DATE-ISSUED: April 6, 2004

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Underwood; Roy Aaron	Long Grove	IL		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Accenture LLP	Palo Alto	CA			02

APPL-NO: 09/ 364164 [PALM]
DATE FILED: July 30, 1999

INT-CL: [07] G06 F 9/44

US-CL-ISSUED: 717/101; 717/120
US-CL-CURRENT: 717/101; 717/120

FIELD-OF-SEARCH: 717/116, 717/100, 717/101, 717/102, 717/108, 717/165, 717/120, 717/223

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4370707	January 1983	Phillips et al.	
☐	5333302	July 1994	Hensley et al.	
☐	5371852	December 1994	Attanasio et al.	
☐	5423032	June 1995	Byrd et al.	
☐	5437027	July 1995	Bannon et al.	
☐	5440719	August 1995	Hanes et al.	
☐	5530829	June 1996	Beardsley et al.	
☐	5623601	April 1997	Vu	
☐	5630069	May 1997	Flores et al.	
☐	5630131	May 1997	Palevich et al.	

☐	5659735	August 1997	Parrish et al.	
☐	5666502	September 1997	Capps	
☐	5673386	September 1997	Batra	
☐	5673387	September 1997	Chen et al.	
☐	5677997	October 1997	Talatik	706/45
☐	5692132	November 1997	Hogan	
☐	5694540	December 1997	Humelsine et al.	
☐	5710884	January 1998	Dedrick	
☐	5724521	March 1998	Dedrick	
☐	5740427	April 1998	Stoller	
☐	5754173	May 1998	Hiura et al.	
☐	5754938	May 1998	Herz et al.	
☐	5754939	May 1998	Herz et al.	
☐	5758062	May 1998	McMahon et al.	
☐	5758074	May 1998	Marlin et al.	
☐	5764897	June 1998	Khalidi	709/201
☐	5778169	July 1998	Reinhardt	
☐	5784553	July 1998	Kolawa et al.	
☐	5812669	September 1998	Jenkins et al.	
☐	5815657	September 1998	Bipinkumar et al.	
☐	5819265	October 1998	Ravin et al.	
☐	5819281	October 1998	Cummins	707/103
☐	5819295	October 1998	Nakagawa et al.	
☐	5835087	November 1998	Herz et al.	
☐	5835911	November 1998	Nakagawa et al.	
☐	5844508	December 1998	Murashita et al.	
☐	5872973	February 1999	Mitchell et al.	709/332
☐	5878432	March 1999	Misheski	
☐	5889520	March 1999	Glaser	
☐	5890161	March 1999	Helland et al.	
☐	5890175	March 1999	Wong et al.	
☐	5892898	April 1999	Fujii et al.	
☐	5930512	July 1999	Boden et al.	
☐	5937165	August 1999	Schwaller et al.	
☐	5949419	September 1999	Domine et al.	
☐	5956732	September 1999	Tsuchida	
☐	5956736	September 1999	Hanson et al.	
☐	5960200	September 1999	Eager et al.	717/147
☐	5995114	November 1999	Wegman et al.	
☐	6014669	January 2000	Slaughter et al.	

☐	6016495	January 2000	Mckeehan et al.	707/103
☐	6029178	February 2000	Martin et al.	
☐	6029195	February 2000	Herz et al.	
☐	6035323	March 2000	Narayen et al.	
☐	6044368	March 2000	Powers	
☐	6055538	April 2000	Kessenich et al.	
☐	6058260	May 2000	Brokel et al.	
☐	6058379	May 2000	Odom et al.	
☐	6061643	May 2000	Walker et al.	
☐	6101503	August 2000	Cooper et al.	
☐	6108670	August 2000	Weida et al.	
☐	6112228	August 2000	Earl et al.	
☐	6112240	August 2000	Pogue et al.	
☐	6115544	September 2000	Mueller	
☐	6137869	October 2000	Voit et al.	
☐	6141010	October 2000	Hoyle	
☐	6141647	October 2000	Meijer et al.	
☐	6151600	November 2000	Derick	
☐	6151610	November 2000	Senn et al.	
☐	6167564	December 2000	Fontana et al.	717/104
☐	6182226	January 2001	Reid et al.	
☐	6185625	February 2001	Tso et al.	
☐	6195794	February 2001	Buxton	
☐	6199068	March 2001	Carpenter	
☐	6199079	March 2001	Gupta et al.	
☐	6202051	March 2001	Woolston	
☐	6208345	March 2001	Sheard et al.	345/356
☐	6209000	March 2001	Klien et al.	
☐	6209033	March 2001	Datta et al.	
☐	6222535	April 2001	Hurd, II	
☐	6223221	April 2001	Kunz	
☐	6230160	May 2001	Chan et al.	
☐	6230194	May 2001	Frailong et al.	
☐	6230309	May 2001	Turner et al.	
☐	6233584	May 2001	Purcell	
☐	6237114	May 2001	Wookey et al.	
☐	6246410	June 2001	Bergeron et al.	
☐	6249905	June 2001	Yoshida et al.	
☐	6256659	July 2001	McLain et al.	
☐	6256678	July 2001	Traughber et al.	

☐	6260068	July 2001	Zalewski et al.	
☐	6266666	July 2001	Ireland et al.	
☐	6272673	August 2001	Dale et al.	
☐	6272678	August 2001	Imachi et al.	
☐	6282605	August 2001	Moore	
☐	6286028	September 2001	Cohen et al.	
☐	6301601	October 2001	Heller et al.	
☐	6304893	October 2001	Gish	
☐	6308188	October 2001	Bernardo et al.	
☐	6313835	November 2001	Gever et al.	
☐	6314434	November 2001	Shigemi et al.	
☐	6327677	December 2001	Garg et al.	
☐	6336118	January 2002	Hammond et al.	
☐	6401085	June 2002	Gershman et al.	
☐	6430556	August 2002	Goldberg et al.	707/4
☐	6438514	August 2002	Hill et al.	703/17
☐	6442620	August 2002	Thatte et al.	
☐	6473794	October 2002	Guheen et al.	709/223

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
0398646	November 1990	EP	
0587394	March 1994	EP	
0643359	March 1995	EP	
WO 98/35297	August 1998	WO	
WO 98/35469	August 1998	WO	
WO 99/01826	January 1999	WO	
WO 01/09752	February 2001	WO	
WO 01/10082	February 2001	WO	

OTHER PUBLICATIONS

Akerley, J., Li N., Parlavecchia A., Programming with VisualAge for Java Version 2, IBM Redbooks, Nov. 1998, pp. 53, 57, 112, 122 295-326.
Anonymous. Optimal Networks Partners With Shomiti Systems to Deliver Extended Application Analysis, press release dated Jul. 14, 1997, three-page text download from.
Behroozi-Toosi et al., "Modeling of Computer Networks and Systems Using SES/Workbench," Proceedings of the Midwest Symposium on Circuits and Systems, May 1991, vol. SYMP. 34, pp. 992-996.
Beta, M., Active Data Objects & ASP, Dr. Dobb's Journal, U.S. M&T Publ., May 1998, vol. 23, No. 5, pp. 88-91, 111-112.
Conradi et al., "Version Models for Software Configuration Management," ACM, pp. 232-282, Jun. 1998.
Dart, S., "Concepts in Configuration Management Systems," ACM, pp. 1-18, 1991.
Dror, A., R. Lafore, "OS/2 Presentation Manager Programming Primer," 1990. McGraw Hill, Berkeley California. Chapter 7, pp. 165-192.
Katzela, Modeling and Simulating Communication Networks: A Hands-O Approach Using OPNET, Mar. 1998, pp. 63-90.

Knutson, "Building the Model Network," Byte, Oct. 1996, vol. 21, No. 10, pp. 101-102, 104.
Law et al., "Stimulation Software for Communications Networks: The State of the Art," IEEE Communications Magazine, Mar. 1994, vol. 32, No. 3, pp. 44-50.
Limprecht, R., "Microsoft Transaction Server," IEEE, Feb. 25, 1997.
Lin et al., "Configuration Management with Logical Structures," ACM, pp. 298-307, 1996.
MIL 3 Inc., "OPNET Tool Operations Manual," 1998, pp. ii-viii, 21Nt-48Nt, 127Pb-143Pb.
Mishra et al., "Effect of Connection Rerouting on Application Performance in Mobile Networks," IEEE Transactions on Computers, vol. 47, No. 4, pp. 371-390. Apr. 1998.
Muller, "Design and Conquer," Byte, Oct. 1996, vol. 21, No. 10, pp. 93-94, 96, 98.
Van Norman, "WAN Design Tools: The New Generation Today's Wide-area Network Design Tools, with Enhanced Tariff Information, Analysis Capabilities and Functions, are Better Than Ever," Data Communications, Oct. 1990, vol. 19, No. 13, pp. 105-106, 108-110, 112.
O'Conner, J., "Internationalization: Localization with ResourceBundles," Java Developer Connection, Online!, Oct. 1998.
Rosove, "Training Requirements for Computer Programmers in Relation to System Development Phases," ACM, Proceedings of the Seventh Annual SIGCPR Conference, pp. 65-76, 1969.
Spitzer, "Tiers Without Tears," DBMS Online, Jan. 12, 1998, pp. 1-5.
Sun Microsystems: "I18N Resource Manager" Sun Documentation, Online!, Apr. 17, 1998, pp. 1-17.
Template Software Inc., Web Componect Foundation Template, Using the Web Component (WEB), 1997, Version 8, Chapters 1-3.
Template Software Inc., Workflow Template Process Template Developing a WFT Workflow System (WFT), 1997, Version 8, Chapters 1-10.
Template Software Inc., "SNAP Foundation Template, Using the SNAP Developement Environment (SNAP DEV)." 1997, Version 8, Chapters 1-11.
Vinoski, "Corba: Integrating Diverse Applications Within Distributed Heterogeneous Environments," IEEE Communications Magazine, Feb. 1997, pp. 46-55.

ART-UNIT: 2122

PRIMARY-EXAMINER: Nguyen-Ba; Hoang-Vu Anthony

ATTY-AGENT-FIRM: Edwards; W. Glenn Oppenheimer Wolff & Donnelly LLP

ABSTRACT:

A system and method are provided for providing an activity framework. First, a plurality of sub-activities are created which each include sub-activity logic adapted to generate an output based on an input received from a user upon execution. Second, a plurality of activities are defined which each execute the sub-activities in a unique manner upon being selected for accomplishing a goal associated with the activity. Selection of one of the activities is allowed by receiving user indicia. An interface is depicted for allowing receipt of the input and display of the output during execution of the sub-activities associated with the selected activity.

24 Claims, 179 Drawing figures

Previous Doc Next Doc Go to Doc#

L16: Entry 8 of 17 File: USPT Apr 6, 2004

DOCUMENT-IDENTIFIER: US 6718535 B1

**** See image for Certificate of Correction ****

TITLE: System, method and article of manufacture for an activity framework design in an e-commerce based environment

Drawing Description Text (25):
FIG. 16A is a flowchart depicting a method for managing user information;

Detailed Description Text (365):
The Membership Directory Manager is used to manage administration and access control for Membership Directory objects, including users and groups, and schema objects. The Membership Directory stores objects used by all Site Server features.

Detailed Description Text (459):
FIG. 16A depicts a method 1600 for managing user information. A site server is provided in operation 1602. The side server has information stored on it including preferences, roles, and details relating to users. A database separate from the site server is provided in operation 1604. The database has information stored thereon including preferences, roles, and details relating to the users. In operation 1606, an identity of one of the users is authenticated. A single interface is displayed in operation 1608, which provides the user access to both the site server and the database upon authentication of the identity of the user. In operation 1610, the user is allowed to view and change the information that is stored on the site server and the database and that is associated with the user. The single interface is tailored in operation 1612 based on the information associated with the user.

Detailed Description Text (475):
With reference to FIG. 16B, the User framework 1630 enables two approaches to maintaining user information. The framework supports two approaches by exposing a single set of interfaces that can be used by either of the two user framework components. With the AFUserSS component 1632, the framework interfaces with the Microsoft Site Server products Personalization and Membership Directory. For this user component, SiteServer holds and manages user information. With the AFUserDB component 1634, the framework interfaces with database tables. For this user component, database tables define the user information.

Detailed Description Text (754):
A component within MTS utilizes role-based security to determine who may or may not have access to a specific COM component. A role is a symbolic name that defines a group of users for a package of components. Roles extend Windows NT security to allow a developer to build secured components in a distributed application.

Detailed Description Text (900):
The web server has static security for each page and security to maintain control of the flow between pages. The static security uses the Windows NT group for each user role to restrict access to each page. For the flow control, the developer uses the Session framework to restrict the ordering of page requests. The allowed ordering of pages are entered into the Session database tables.

Detailed Description Text (1123):
Who needs access to the application, i.e. what is your user group? Is it all Internet users or some authorized subset? Does one only have one type of user or are multiple levels of authorization required?

Detailed Description Text (1594):

Select Intranet [Windows NT Authentication] Membership option. Next create the sample site. Right click on the "Computer name" under the Commerce Host Administration folder (Refer to FIG. 62--Computer Name is "ZIMMERD3" 6208). Select New--Commerce Site Foundation. Create New Site Foundation Wizard 6300 appears. FIG. 63 is an illustration of a Create New Site Foundation Wizard. Select to create site on "Site Server Commerce Membership Samples Web Site" option 6302. Follow steps in the wizard. After Site has been created, right click on Default Web Site in Internet Information Server, select Task--Membership Server Mapping . . . Change the Membership Server Mapping back to "Commerce Membership Server".

Detailed Description Text (2911):
Multilevel Security: PVCS allows security by user, group and archive.

Detailed Description Paragraph Table (70):
Title Description & Responsibilities Technical Typically an IS department head with responsibility for Manager the purchase and/or support of hardware and software. In configuration management, this role is more software oriented. Other responsibilities include: Assign development and support staff to projects. Review (accept/reject) technical approach proposed for projects. Monitor development and support budgets and personnel-status of projects. Network System This individual is responsible for the installation, Administrator maintenance and support of the Unix and Windows NT servers including operating system, file systems, and applications. Other responsibilities include: Operating system installation, patch updates, migrations and compatibility with other applications. Installation and support of proper backup/restore systems. Installation and support of other peripherals required for installed (or to be installed) applications. Proper portion of the present description of hardware configuration and setup. Maintenance of Windows Domain users and Groups as well as other security issues. Database The DBA is responsible for proper creation and Administrator maintenance of production and system test databases. The integrity of the database, as well as recovery using backup/restore and logging, are priorities for the DBA. Other responsibilities include: Assist developers in maintaining development databases by automating backup/recovery, applying changes to database schema, etc. Provide support for tuning, sizing and locating database objects within allocated database space. Applying change requests to databases. Ideally maintain entity relationship diagrams for databases. Maintenance of database users and other database- related security issues Source Code Individual responsible for development and Librarian maintenance of source code control tools, training materials, and storage areas. The Source Code Librarian is also responsible for the integrity of the source code environment. Additionally: Establishes source code directories for new projects. Provides reports on source code environment status and usage per project. Provides assistance/information as needed regarding objects to check out for system test. Assists production operations in building/moving all applications into production. Business Analyst Individual or individuals responsible for managing the detailed design, programming, and unit testing of application software. Other responsibilities include: Developing/reviewing detailed designs. Developing/reviewing unit test plans, data, scripts, and output. Managing application developers. Application Individual or individuals responsible for making Developer changes to source code defined by management. This person typically: Checks source code out of the source code environment. Modifies code per user requirements or other development portion of the present description. Unit tests modifications in the development environment. Checks modified code back into source code environment in preparation for system test. System Tester This person or team is directly responsible for system Integration Tester testing or integration testing of an application prior to implementing in production. This may also take the form of performance testing. Typically, a system or integration test person or team may be responsible for: Following production operation procedures for installing a new application in the appropriate test environment. Develop and execute a test plan to properly exercise new application including new, modified, and unmodified functionality. Reporting results of test. Vendor For the purposes of this portion of the present description, a vendor is defined as an organization from which software has been purchased for use by the clients systems. Alternatively, a vendor may distribute final installable media in the form of tape or CD with upgrades or new release of application. A vendor may: Make modifications to application code at vendor offices or within the engagement development environment. Provide necessary information to Source Code Librarian to store new code. Assist Source Code Librarian in transferring modifications to the engagement system test environment. Participate in system test (or performance test).